## In the Claims

The status of claims in the case is as follows:

[Previously presented] A method of operating a virtual 1 private network (VPN) based on IP Sec that integrates 2 network address translation (NAT) with IP Sec processing, 3 comprising the steps executed at one end of a VPN connection 5 of: configuring a NAT IP address pool; 6 configuring a VPN connection to utilize said NAT IP 7 address pool; 8 obtaining a specific IP address from said NAT IP 9 address pool, and allocating said specific IP address 10 for said VPN connection; 11 starting said VPN connection; 12 loading to an operating system kernel the security 13 associations and connection filters for said VPN 14

2

S/N 09/578,215

END919990129US1

- .15 connection;
- processing a IP datagram for said VPN connection; and
- 17 applying VPN NAT to said IP datagram.
  - 1 2. [Original] The method of claim 1, wherein said VPN
  - connection is configured for outbound processing, and said
  - 3 applying step comprises outbound source IP Nating.
  - 3. [Original] The method of claim 1, wherein said VPN
  - 2 connection is configured for some combination of inbound
  - 3 processing, and said applying step selectively comprises
  - 4 inbound source IP NATing or inbound destination IP NATing.
  - 1 4. [Original] The method of claim 1, further for
  - 2 integration of NAT with IP Sec for manually-keyed IP Sec
  - 3 connections, comprising the further step of manually
  - 4 configuring connection keys.
  - 5. [Original] The method of claim 1, further for
  - 2 integrating NAT with IP sec for dynamically-keyed (e.g. IKE)
  - 3 IP Sec connections, comprising the further step of:

END919990129US1

S/N 09/578,215

3

- 4 configuring the VPN connections to obtain their keys
- 5 automatically.
- 1 6. [Original] The method of claim 1, further for
- 2 integrating NAT with IP Sec Security Associations,
- 3 negotiated dynamically by IKE, wherein said starting step
- 4 further comprises creating a message for IKE containing said
- 5 IP address from said NAT pool; and further comprising the
- step of operating IKE to obtain dynamically negotiated keys.
- 1 7. [Original] The method of claim 6, further comprising
- 2 the step of combining the dynamically obtained keys with
- 3 said NAT pool IP address and wherein said loading step loads
- 4 the result as security associations into said operating
- 5 system kernel.
- 8. [Currently amended] A method for allowing the
- 7 definition and configuration of NAT directly with definition
- 8 and configuration of IPsec-based VPN connections and VPN
- 9 policy, comprising the steps executed by a digital processor
- 10 at one end of a VPN connection of:
- configuring the requirement for VPN NAT by a yes/no
- decision in a policy database for each of the three

END919990129US1

13 typ	es of	VPN	NAT,	said	three	types	being	$\mathbf{v}_{\mathbf{P}\mathbf{N}}$	NAT	type	а
--------	-------	-----	------	------	-------	-------	-------	-------------------------------------	-----	------	---

- 14 outbound source IP NAT, VPN NAT type c inbound source
- 15 IP NAT, and VPN NAT type d inbound destination IP NAT;
- 16 and
- configuring a remote IP address pool or a server IP
- address pool selectively responsive to said yes/no
- 19 decision for each said VPN NAT type.
- 9. [Original] The method of claim 8, further comprising
- 2 the step of configuring a unique said remote IP address pool
- 3 for each remote address to which a VPN connection will be
- 4 required, whereby said remote IP address pool is keyed by a
- 5 remote ID.
- 1 10. [Original] The method of claim 8, further comprising
- 2 the step of configuring said server IP address pool once for
- 3 a system being configured.
- 1 11. [Previously presented] A method of providing customer
- 2 tracking of VPN NAT activities as they occur in an operating
- 3 system kernel, comprising the steps executed at one end of a
- 4 VPN connection of:

END919990129US1

5	responsive to VPN connection configuration, generating
6 .	journal records;
7	updating said journal records with new records for eac
8	datagram processed through a VPN connection; and
9	enabling a customer to manage said journal records.
1.	12. [Currently amended] A method of allowing a VPN NAT
2	address pool to be associated with a gateway, thereby
3	allowing server load- balancing, comprising the steps
4	executed by a digital processor at one end of a VPN
5	connection of:
6	configuring a server NAT IP address pool for a system
7	being configured;
8	storing specific IP addresses that are globally
9	routable in said server NAT IP address pool;
10	configuring a VPN connection to utilize said server NA
11	IP address pool; and
12	managing total volume of concurrent VPN connections
	END919990129US1 6 S/N 09/578,215

13	responsive	to th	e number	of	addresses	in	said	server
14	NAT IP add	cess p	ool.					

- 1 13. [Previously presented] A method of controlling the
- 2 total number of VPN connections for a system based on
- 3 availability of NAT addresses, comprising the steps executed
- 4 at one end of a VPN connection of:
- configuring the totality of remote IP address pools
  with a common set of IP addresses, said addresses being
  configured as a range, as a list of single addresses,
  or any combination of multiple ranges and single
- 9 addreses; and
- limiting the successful start of concurrently active

  VPN connections responsive to the number of said IP

  addresses configured across the totality of said remote

  address pools.
  - 1 14. [Previously presented] A method of performing virtual
  - 2 private network (VPN) network address translation on
- 3 selected ICMP datagrams, comprising the steps executed at

7

4 one end of a VPN connection of:

END919990129US1

5 c	ombining	ΙP	Security	&	NAT	bу	detecting	selected	types
-----	----------	----	----------	---	-----	----	-----------	----------	-------

- of ICMP type packets; and
- 7 responsive to said selected types, performing network
- address translation functions on the entire datagram
- 9 including ICMP data.
- 1 15. [Previously presented] A method of performing virtual
- 2 private network (VPN) network address translation on
- 3 selected FTP datagrams, comprising the steps executed at one
- 4 end of a VPN connection of:
- 5 combining IP Security & NAT by detecting the occurrence
- of FTP PORT or PASV FTP commands; and
- 7 responsive to said command, performing network address
- 8 translation on the FTP data and the header.
- 1 16. [Currently amended] A system for operating a virtual
- 2 private network (VPN) based on IP Sec that integrates
- 3 network address translation (NAT) with IP Sec processing
- 4 executed by a digital processor at one end of a VPN
- 5 connection, comprising:

END919990129US1 8 S/N 09/578,215

6	means for configuring a NAT IP address pool;
7	means for configuring a VPN connection to utilize said
<b>8</b>	NAT IP address pool;
9	means for obtaining a specific IP address from said NAT
10	IP address pool, and allocating said specific IP
11	address for said VPN connection;
12	means for starting said VPN connection;
13	means for loading to an operating system kernel the
14	security associations and connection filters for said
15	VPN connection;
16	means for processing a IP datagram for said VPN
17	connection; and
18	means for applying VPN NAT to said IP datagram.
1	17. [Currently amended] A system for definition and
2	configuration of NAT directly with definition and
3	configuration of VPN connections and VPN policy executed by
4	a digital processor at one end of a VPN connection,
	END919990129US1 9 S/N 09/578,215

5 comprising:

Mar 14 2005 12:41

- a policy database for configuring the requirement for
- 7 VPN NAT by a yes/no decision for each of the three
- 8 types of VPN NAT, said three types being VPN NAT type a
- outbound source IP NAT, VPN NAT type c inbound source
- 10 IP NAT, and VPN NAT type d inbound destination IP NAT;
- 11 and
- a remote IP address pool or a server IP address pool
- selectively configured responsive to said yes/no
- 14 decision for each said VPN NAT type.
- 1 18. [Previously presented] A system implemented at one end
- 2 of a VPN connection for allowing a VPN NAT address pool to
- 3 be associated with a gateway, thereby allowing server
- 4 load-balancing, comprising:
- a server NAT IP address pool configured for a given
- 6 system being configured for containing multiple address
- 7 configured as a range, as a list of single addresses,
- 8 or any combination multiple ranges and single
- 9 addresses;

END919990129US1

10

10	said server NAT IP address pool storing specific IP
11	addresses that are globally routable;
12	a VPN connection configured to utilize said server NAT
13	IP address pool; and
14	a connection controller for managing total volume of
15	concurrent VPN connections responsive to the number of
16	addresses in said server NAT IP address pool.
1	19. [Previously presented] A program storage device
2	readable by a machine, tangibly embodying a program of
3	instructions executable by a machine to perform method steps
4	executed at one end of a VPN connection for operating a
5	virtual private network (VPN) based on IP Sec that
6	integrates network address translation (NAT) with IP Sec
7	processing, said method steps comprising:
8	configuring a NAT IP address pool;
9	configuring a VPN connection to utilize said NAT IP
10	address pool;
11	obtaining a specific IP address from said NAT IP
	END919990129US1 11 S/N 09/578,215

S/N 09/578,215

12		address pool, and allocating said specific IP address
13		for said VPN connection;
14		starting said VPN connection;
15		loading to an operating system kernel the security
16		associations and connection filters for said VPN
17		connection;
18	-	processing a IP datagram for said VPN connection; and
19		applying VPN NAT to said IP datagram.
1	20.	[Previously presented] An article of manufacture
2	comp	orising:
3		a computer useable medium having computer readable
4		program code means embodied therein for operating a
5		virtual private network (VPN) based on IP Sec that
6		integrates network address translation (NAT) with IP
7		Sec processing executed at one end of a VPN connection
8		the computer readable program means in said article of
9		manufacture comprising:

12

END919990129US1

10	computer readable program code means for causing a
11	computer to effect configuring a NAT IP address pool;
12	computer readable program code means for causing a
13	computer to effect configuring a VPN connection to
14	utilize said NAT IP address pool;
15	computer readable program code means for causing a
16	computer to effect obtaining a specific IP address from
17	said NAT IP address pool, and allocating said specific
18	IP address for said VPN connection;
19	computer readable program code means for causing a
20	computer to effect starting said VPN connection;
21	computer readable program code means for causing a
22	computer to effect loading to an operating system
23	kernel the security associations and connection
24	filters for said VPN connection;
25	computer readable program code means for causing a
26	computer to effect processing a IP datagram for said
27	VPN connection; and

END919990129US1 13

28	computer readable program code means for causing a
29	computer to effect applying VPN NAT to said IP
30	datagram.
·1	21. [Currently amended] Method for providing IP security
, 2	in a virtual private network using network address
3	translation (NAT), comprising the steps executed $\underline{by}$ a
4	digital processor at one end of a VPN connection of:
5	dynamically generating NAT rules and associating them
6	with manual or dynamically generated (IKE) Security
7	Associations; thereafter
8	beginning IP security that uses the Security
9	Associations; and then
10	as IP Sec is performed on outbound and inbound
11	datagrams, selectively performing one or more of VPN
12	NAT type a outbound source IP NAT, VPN NAT type c
13	inbound source IP NAT, and VPN NAT type d inbound
14	destination IP NAT.
1	22. [Original] The method of claim 1, said NAT IP address
2	pool containing multiple addresses configured as a range, as
	ENDO: 0000120US1 14 S/N 09/578.215

- a list of single address, or any combination of multiple
- ranges and single addresses.